(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification⁷: H04Q 7/32, G06K 7/00

(21) International Application Number:
PCT/NO2005/000102

(22) International Filing Date: 21 March 2005 (21.03.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20041347   31 March 2004 (31.03.2004)   NO

(71) Applicant (for all designated States except US): TE-LENOR ASA [NO/NO]; Snarøyveien 30, N-1331 Fornebu (NO).

(72) Inventors; and
(75) Inventors/Applicants (for US only): CALVET, Juan,

Carlos López [MX/NO]; Hovseterveien 66C, N-0768 Oslo (NO). NOLL, Josef [DE/NO]; Linjeveien 6, N-1084 Oslo (NO).

(74) Agent: ONSAGERS AS; P.O. Box 6963 St. Olavs plass, N-0130 Oslo (NO).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
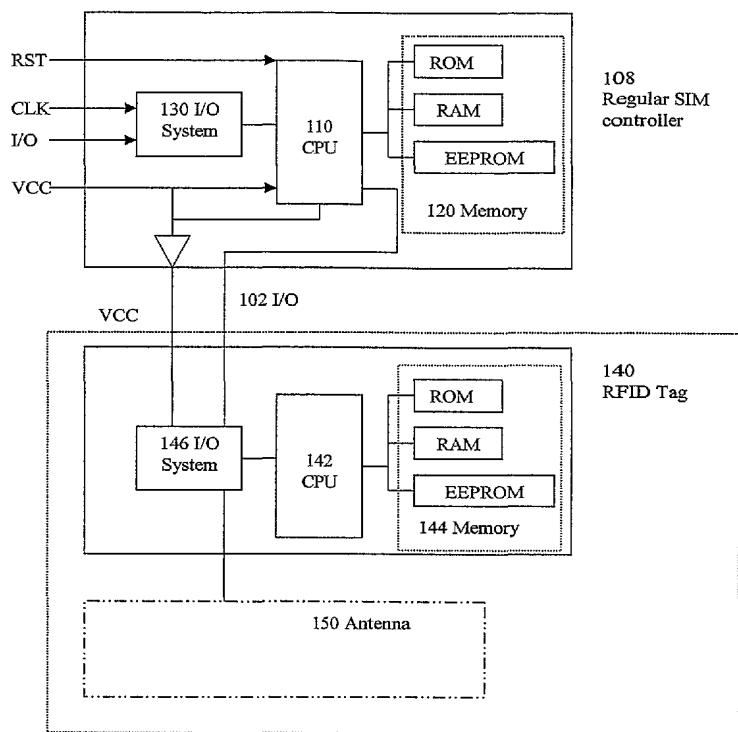
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,

[Continued on next page]

(54) Title: SUBSCRIBER IDENTITY MODULE

100 SIM card

(57) Abstract: The invention relates to a subscriber identity module for a mobile communication terminal, comprising a processing device, a memory device, an I/O device and a wireless communication device, in particular an interrogatable transponder such as an RFID transponder. The RFID transponder is operatively controllable by said processing device, and comprises a memory which contains identification data, configurable by the processing device. The RFID-enabled subscriber identification module may be used as an authentication token. A method for providing secure communications between the subscriber identification module and an RFID interrogating device is also provided.

ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SUBSCRIBER IDENTITY MODULE

Technical field

The present invention relates in general to mobile communication, wireless security
and authentication. More specifically, the invention relates to a subscriber identity
module for a mobile communication terminal, and a mobile communication terminal
comprising such a subscriber identity module. The invention also relates to a
method for providing secure data communication between a subscriber identity
module and an external communication device, for execution by such a subscriber
identity module, and to uses of a subscriber identity module or a mobile terminal
equipped with such a module for authentication purposes.

Background of the invention

A subscriber identity module, or SIM card, is a removable module for use with
mobile communication terminals, such as GSM mobile telephones. The SIM card
contains subscriber specific data and is, in use, accessible by the central processing
unit of the mobile terminal. The SIM card typically also comprises features for
authenticating a user/subscriber. The SIM card includes a processing unit, a
memory device and I/O devices for communication with the processing unit of the
mobile terminal. The memory device contains a subscriber authentication key and
computer program instructions for causing the SIM card processing unit to
authenticate the user/subscriber.

WO-03/081934 discloses a mobile telephone provided with a SIM card. The mobile
telephone is also provided with an RFID tag for authentication purposes. User-
specific, interrogatable information is written into the RFID tag by means of the
mobile telephone's processing unit. As the RFID tag is attached to the mobile
telephone, only a mobile telephone having this built-in feature can be used for
authentication.

WO-98/58509 discloses a mobile phone provided with a SIM card. The SIM card is
further provided with a wireless interface or communication module, providing data
transmission between the SIM card and an external device such as another SIM card
in another mobile telephone, a computer or a cash register. This related background
art provides for a separate communication channel between the external device and
the SIM card. However, the publication apparently does not indicate a solution for
making the SIM card interrogatable by an external interrogating device.

None of the publications appear to disclose a simple, effective and reliable solution
for using the SIM card as a remotely activated authentication device.

None of the publications appear to disclose a simple, effective and reliable method for providing secure wireless data communication between the subscriber identity module and an external interrogating device.

Summary of the invention

An objective of the present invention is to provide a subscriber identity module, a mobile terminal and a method for providing secure data communication between a subscriber identity module and an external interrogating device, whereby at least some of the above mentioned drawbacks of the related background art are overcome.

In accordance with a first aspect of the present invention, there is provided a subscriber identity module as indicated in the appended independent claim 1.

In accordance with a second aspect of the present invention, there is provided a mobile communication terminal as indicated in the appended independent claim 16.

In accordance with a third aspect of the present invention, there is provided a method for providing secure data communication between a subscriber identity module and an interrogating device, as indicated in the appended independent claim 20.

The invention also relates to the use of a subscriber identity module as an authentication token, as indicated in claims 13-15.

The invention also relates to the use of a mobile communication terminal as an authentication token, as indicated in claims 17-19.

Further advantageous embodiments of the invention are set forth in the dependent claims.

Additional features and principles of the present invention will be recognized from the detailed description below.

It is to be understood that both the foregoing general description and the following detailed description are exemplary and explanatory only and are not restrictive of the invention, as claimed.

Brief description of the drawings

The accompanying drawings illustrate a preferred embodiment of the invention. In the drawings,

Fig. 1 is a schematic block diagram illustrating a first embodiment of a subscriber identity module according to the invention,

Fig. 2 is a schematic block diagram illustrating a second embodiment of a subscriber identity module according to the invention,

Fig. 3 is a schematic block diagram illustrating a system for merging RFID and mobile communication services, enabled by the present invention, and

5   Fig. 4 is a flowchart illustrating a method according to the invention,

Fig. 5 is a schematic block diagram illustrating the physical layout of a subscriber identity module according to the invention, and

Fig. 6 is a schematic block diagram illustrating an analog front end module for connecting the antenna and the SIM/RFID controller.

10   **Detailed description of the invention**
Fig. 1 is a schematic block diagram illustrating a first embodiment of a subscriber identity module according to the invention.

Fig. 1 illustrates a "bi-card" embodiment, wherein the SIM card 100 comprises separate processing devices, memory devices and I/O devices for the regular SIM
15   functionality and the RFID functionality, respectively.

The SIM card 100 is arranged for use with a mobile communication terminal (not illustrated) such as a GSM enabled mobile telephone. The SIM card 100 comprises a processing device 110, a memory device 120, an I/O device 130, corresponding to a regular SIM controller 108 with regular SIM functionality.

20   The I/O device 130 comprises an interface between the SIM card and the mobile communication terminal, typically including electric connections provided on the surface of the SIM card.

The memory device 120 may comprise volatile and non-volatile memory portions, such as, e.g., RAM, ROM, EEPROM, and Flash memory.

25   The SIM card 100 also comprises a wireless communication device 140, in particular an interrogatable transponder 140.

The interrogatable transponder 140 is an active RFID tag. The transponder 140 is operatively controllable by the processing device 110, indicated by the line referred to by I/O. This communication line between the processing unit 110 and the
30   transponder 140 enables the SIM card 100 to trigger events in the RFID tag and vice versa. It could also transmit certain amounts of data.

In particular, the power of the transponder 140 is controlled by the processing device 110, giving the possibility of turning the tag on and off as desired, operatively controlled by the processing device 110.

4

More specifically, the transponder may be operatively enabled or disabled, controlled by an on/off signal provided by the mobile communication terminal via the I/O device 130.

5   In one embodiment, the on/off signal is provided by a user via a user interface, such as a keyboard, in the mobile terminal. In another embodiment, the on/off signal is provided to the mobile communication terminal by a mobile communication operator, in particular by a command transmitted to the mobile communication terminal by the operator.

10   In either case, the resulting remote enabling/disabling function of the RFID tag involves a security improvement, as the existing problem of tracing or copying continuously activated RFID tags may be overcome or reduced.

The transponder 140 comprises identification data contained in a memory 144. The identification data may be configured or set by the processing device 110.

15   In particular, the identification data is provided to the transponder by the mobile communication terminal via the I/O device 130.

The identification data is preferably transmitted to the mobile communication terminal by a mobile communication operator.

By this feature, the identification data stored in the RFID tag may be changed or re-written with new data supplied and transmitted by the mobile communication
20   operator. This leads to the useful result that if the RFID tag is illegally/fraudulently copied, the operator will have the possibility of writing a new ID into the RFID tag without having to physically change the SIM card.

The memory 144 may comprise volatile and non-volatile memory portions, such as, e.g., RAM, ROM, EEPROM, and Flash memory.

25   When the transponder 140 is interrogated by an external interrogating RF device (not illustrated), the transponder 140 is arranged to transmit, via the antenna 150, a RF signal coded with the identification data contained in the memory 144.

Fig. 2 is a schematic block diagram illustrating a second embodiment of a subscriber identity module according to the invention.

30   This embodiment mainly corresponds to the embodiment illustrated in fig. 1. However, the transponder comprises an antenna, and the RFID transponder functionality is implemented by means of the processing device, the memory device and the I/O device that are included in the subscriber identity module, i.e. the controller components also used for the regular SIM functionality.

Fig. 2 thus illustrates a "hybrid-card" embodiment, wherein the SIM card 200 comprises a processing device 210, memory devices 220 and I/O devices 230 which are shared between the regular SIM functionality and the RFID functionality.

The SIM card 200 is arranged for use with a mobile communication terminal (not illustrated) such as a GSM enabled mobile telephone.

The memory device 220 may comprise volatile and non-volatile memory portions, such as, e.g., RAM, ROM, EEPROM, and Flash memory.

The SIM card 200 also comprises a wireless communication device 140, in particular an interrogatable transponder 140, comprising an antenna 250 and the RFID functionality provided by the processing device 210, the memory devices 220 and the I/O devices 230.

The interrogatable transponder 240 constitutes an active RFID tag, operatively controllable by the processing device 210.

The transponder 240 comprises identification data contained in the memory 220. The identification data may be configured or set by the processing device 210.

When the transponder 240 is interrogated by an external interrogating RF device (not illustrated), the transponder 240 is arranged to transmit, via the antenna 250, a RF signal coded with the identification data contained in the memory 220.

This second embodiment is made possible since the basic architecture of both active RFID tags and SIM cards are so similar. This embodiment proposes a slightly more powerful SIM card controller with an external RFID antenna. In this case there is no need for communication between two separate cards or modules. As appears from fig. 2, the antenna 250 is external to the SIM/RFID controller 208, but still integrated on the SIM card 200.

Fig. 3 is a schematic block diagram illustrating a system for merging RFID and mobile communication services, enabled by the present invention.

A mobile terminal 300, such as a mobile telephone 300, is provided with a subscriber identity module as disclosed above.

The mobile terminal 300 brings many new opportunities by merging the services typically provided by RFID tags with the infrastructure provided by GSM.

The idea is that events initiated by the RFID will trigger events in the mobile phone and its services, and vice versa.

Adopting the RFID technology in the SIM cards used in mobile phones avoids many practical problems that IrDA and Bluetooth have, such as pairing and alignment, bringing a fast, easy and secure way to wirelessly interact with other systems.

Fig. 4 is a flow chart illustrating a method according to the invention.

5   The method is a Public Key Infrastructure (PKI) based process for execution by a subscriber identity module, i.e. for execution by the processing device in such a subscriber identity module, according to the invention. The purpose of the method is to provide secure data communication between the subscriber identity module and an external interrogating device, such as, e.g., a RFID reader (an RFID
10   communication/interrogation device) of a door access system.

The method utilizes a private key stored in SIM card with the purpose of providing a secure communication between the external communication device and the RFID transponder included in the SIM card. This means that the RFID transponder and thus the RFID enabled SIM card can make use of the entire PKI infrastructure that
15   is already behind the SIM card to increase the communication security between the RFID tag and the reader.

When a RFID transponder identifies itself to an external reader, the reader will then have enough information to retrieve the correspondent mobile phone's public key in order to start a communication session with the tag and possibly exchange a shared
20   key to encrypt further communication between the tag and the reader.

The subscriber identity module or SIM card is operatively arranged in a mobile terminal such as a GSM mobile telephone. The SIM card comprises, in accordance with the detailed description of one of the embodiments disclosed in fig. 1 or fig. 2 above, a processing device, a memory device containing a private key, an I/O
25   device, and an interrogatable transponder.

The method starts at the initiation step 400. The method further comprises the following steps, preferably performed in the indicated order:

In step 410, the RFID part of the SIM card is interrogated by the external interrogating device. Upon this interrogation, as a result of the interrogation, the
30   SIM card transmits the identification data.

Next, in step 420, an encrypted message is received from the external communication device. The message is encrypted with a public key associated with the identification data transmitted in the foregoing step 410. The public key is provided by the external interrogating device, preferably by a search in a database,
35   in order to match the identification with the corresponding public key.

Next, in step 430, the encrypted message is decrypted using the private key.

Next, in step 440, the decrypted message is used as a shared key.

In step 450 this shared key is used to encrypt further data communication between the subscriber identity module and the external interrogating device.

5   In particular, the encryption is performed by using a predetermined symmetric key algorithm such as 3DES, which is supported by the SIM card and the reader.

Fig. 5 is a schematic block diagram illustrating the physical layout of a subscriber identity module according to the invention.

Fig. 5 illustrates an exemplary layout of the "hybrid-card" embodiment 200 of the subscriber identity module according to the invention, as described above with
10   reference to fig. 2. The skilled person will realize that a similar layout also could be used for the "bi-card" embodiment 100 described above with reference to fig. 1.

The physical dimensions and connection terminals of the SIM card 200 is preferably designed in accordance with the starndards GSM 11.11 and ISO 7816, and thus, they are not further described in the present specification. The antenna 250 is
15   realised as a wire loop extending along the edge of the card 200, preferably as a multiturn loop. The number of turns is preferably 3, as illustrated in fig. 5. The antenna 250 is connected to the analog front-end module 252 (not shown in fig. 2), which is further described below with reference to fig. 6. The analog front-end module 252 is further connected to the integrated SIM card processor 208.

20   Fig. 6 is a schematic block diagram illustrating the principles of an exemplary analog front end module 252 for connecting the antenna and the SIM/RFID controller. The analog front end module 252 comprises an MOS transistor NMOS connected in parallel with the antenna input ANT1, ANT2. Another MOS transistor PMOS is connected between the voltage supply VCC and the voltage supply input
25   of the comparator COMP. The gate of the NMOS transistor and the gate of the PMOS transistor are both connected to the control signal MOD. During receiving of data from the antenna the MOS transistors are turned off by setting the control signal MOD low. Then the signal received by the antenna is demodulated by the diode D and the capacitor C and fed to the comparator COMP to bring the signal up
30   to a derived signal DATA with correct level. The reference level REF of the comparator is chosen as appropriate.

Use examples

The following examples illustrate useful applications for the present invention.

Access control use

35   The SIM card according to the invention may be used as an authentication token for an access control system. Likewise, a mobile terminal which includes a SIM card

according to the invention may also be used as an authentication token for an access control system.

In such an exemplary use scenario, a mobile phone equipped with an RFID enabled SIM card according to the invention is detected by an RFID reader at a door which

5   is provided with an access control system. A number received by the RFID reader at the door is recognized in the access control system as a valid number, which means that the mobile telephone is a registered telephone in the access control system. The access control system will then send a challenge to the phone via the GSM network. The user is asked to type a PIN number, if the PIN number is correct a signal is sent

10   via RFID and the door is opened. In this case the user is authenticated with something he has (mobile phone with RFID tag) with something he has (PIN number).

Mobile commerce use

The SIM card according to the invention may be used as an authentication token for

15   a mobile commerce system such as the Telenor MobilHandel. Likewise, a mobile terminal which includes a SIM card according to the invention may also be used as an authentication token for such a mobile commerce system.

In such an exemplary use scenario, a user, provided with a mobile phone equipped with an RFID enabled SIM card according to the invention, is located in front of a

20   cash register in a commerce establishment. After deciding which good he wants to purchase, the RFID tag in the mobile phone is read by the machine, and since the machine now knows to which phone number this tag belongs to, a request for purchase is sent via GSM using a M-Commerce service to the mobile phone. The user will then accept the transaction typing his PIN number, which is then sent back

25   to the M-Commerce service and back to the cash register where the goods are dispensed.

In both above cases the RFID tag number is directly linked with the mobile phone number in a central database. So whenever the tag is detected most of the services provided by a mobile phone can potentially be used.

30   The SIM card according to the invention, or a mobile terminal which includes a SIM card according to the invention, may be used as an authentication token for other purposes as well.

Electronic key scenario

In an electronic key scenario, an electronic key is sent to a mobile phone through an

35   SMS. A door is controlled by an access control system which is configured to recognize an RFID enabled SIM card in a mobile telephone, according to the invention. The access control system is further configured to recognize the

electronic key when the mobile phone is present. When the user arrives at the door, holding the mobile phone which exposes both values (key and RFID number) the door will automatically be opened.

Security and privacy use

5   When a mobile phone is stolen, the RFID enabled SIM card can be deactivated remotely, avoiding any possible misuse. The RFID enabled SIM card could also be deactivated through the mobile phone to avoid been detected when this is not wanted.

Business issues

10   The invention solves a problem for any business that wishes to adopt the RFID technology, in a way that there will not be a need to distribute RFID cards to the user, because potentially everyone with a mobile phone will already have a card.

Users will also benefit from such solution in a way that they will only need to carry their mobile phones in order to authenticate towards different services.

15 . As most of the services offered by mobile phones, one of the biggest barriers to adopt the solution is that the market penetration has to be big enough to present an attractive alternative to already established businesses. This means that the solution should be able to function properly in all the mobile phones, and this is never an easy task.

20   Users will also have to renew their SIM cards, and this is implies a cost for Mobile Operators.

The above detailed description has explained the invention by way of example. A person skilled in the art will realize that numerous variations and alternatives to the detailed embodiment exist within the scope of the invention, as set forth by the

25   appended claims.

CLAIMS

1.   Subscriber identity module for a mobile communication terminal, comprising a processing device, a memory device, an I/O device and a wireless communication device,

5   characterized in that said wireless communication device is an interrogatable transponder.

2.   Subscriber identity module according to claim 1,
wherein said interrogatable transponder is operatively controllable by said processing device.

10   3.   Subscriber identity module according to claim 2,
wherein the transponder is arranged to be operatively enabled or disabled, controlled by a signal provided by the mobile communication terminal via said I/O device.

4.   Subscriber identity module according to claim 3,
15   wherein said signal is provided by a user interface in the mobile terminal.

5.   Subscriber identity module according to claim 4,
wherein said signal is provided by a mobile communication operator.

6.   Subscriber identity module according to claim 2,
wherein said interrogatable transponder comprises identification data contained in a
20   memory, said identification data being configurable by said processing device.

7.   Subscriber identity module according to claim 6,
wherein said identification data is provided by the mobile communication terminal via said I/O device.

8.   Subscriber identity module according to claim 7,
25   wherein said identification data is provided by a mobile communication operator.

9.   Subscriber identity module according to claim 3,
wherein said interrogatable transponder is arranged to transmit a RF signal coded with said identification data when interrogated by an external interrogating RF device.

30   10.   Subscriber identity module according to one of the claims 1-9,
wherein said transponder is an active RFID transponder.

11.   Subscriber identity module according to claim 10,
wherein said transponder is a separate device, comprising a processing device, a memory device and an I/O device connected to an antenna.

12.   Subscriber identity module according to claim 10,
wherein said transponder comprises an antenna, and wherein further RFID
transponder functionality is implemented by means of the processing device and the
memory device included in said subscriber identity module.

13.   Use of a subscriber identity module according to one of the claims 1-12, as
an authentication token.

14.   Use of a subscriber identity module according to one of the claims 1-14, as
an authentication token for an access control system.

15.   Use of a subscriber identity module according to one of the claims 1-12, as
an authentication token for a mobile commerce system.

16   Mobile communication terminal, comprising a subscriber identity module
according to one of the claims 1-12.

17.   Use of a mobile communication terminal, comprising a subscriber identity
module according to one of the claims 1-12, as an authentication token.

18.   Use of a mobile communication terminal, comprising a subscriber identity
module according to one of the claims 1-12, as an authentication token for an access
control system.

19   Use of a mobile communication terminal, comprising a subscriber identity
module according to one of the claims 1-12, as an authentication token for a mobile
commerce system.

20.   Method for execution by a subscriber identity module, for the purpose of
providing secure data communication between the subscriber identity module and
an external interrogating device, said subscriber identity module comprising a
processing device, a memory device containing a private key, an I/O device, and an
interrogatable transponder,
said method comprising the steps of
- transmitting identification data upon an interrogation by the external interrogating
device,
- receiving an encrypted message from the external communication device, said
message being encrypted with a public key associated with said identification data,
- decrypting said encrypted message using said private key,
- using the decrypted message as a shared key to encrypt further data
communication between the subscriber identity module and the external
interrogating device.

21.   Method according to claim 20,
wherein said public key is provided by said external interrogating device by

searching a database in order to match said identification with the corresponding public key.
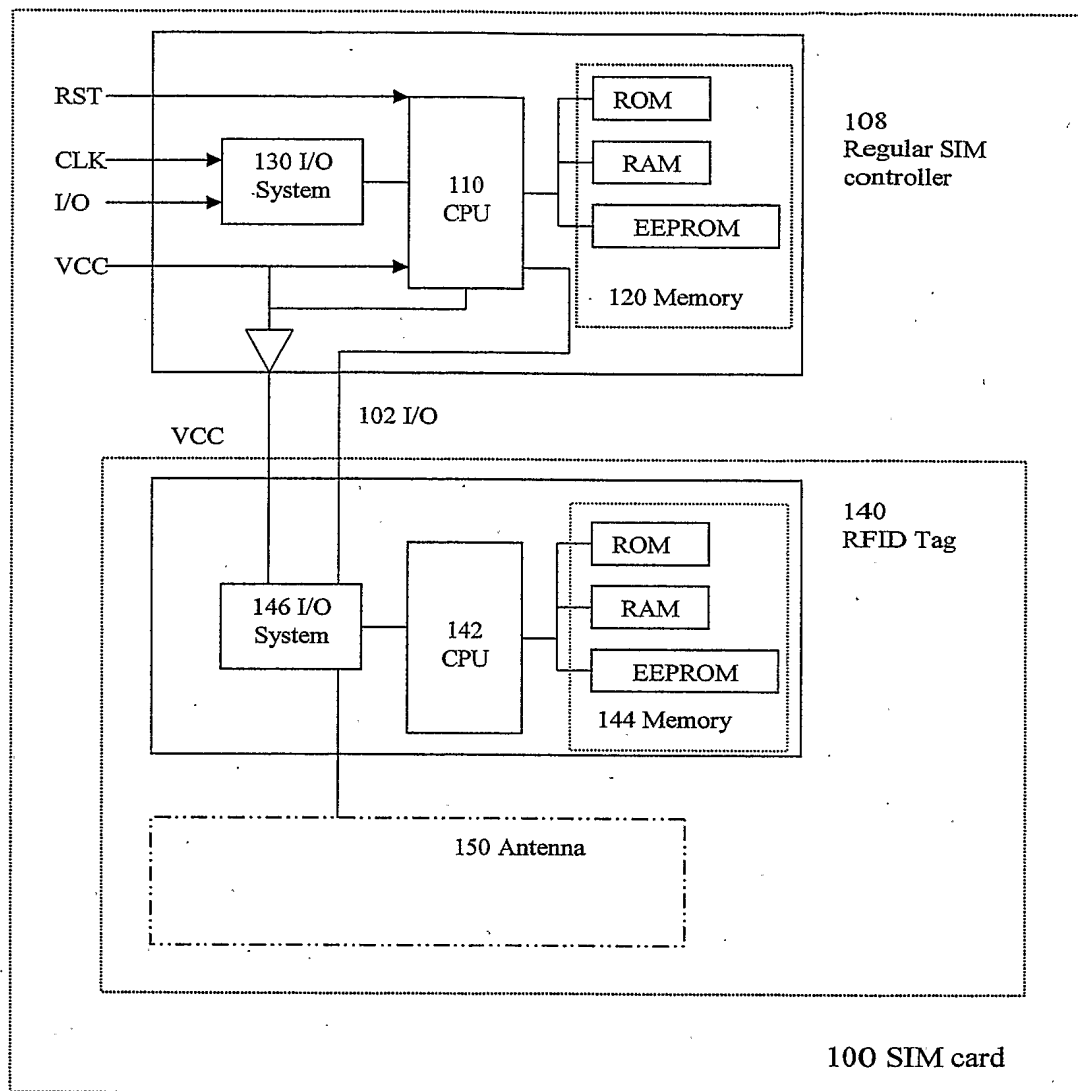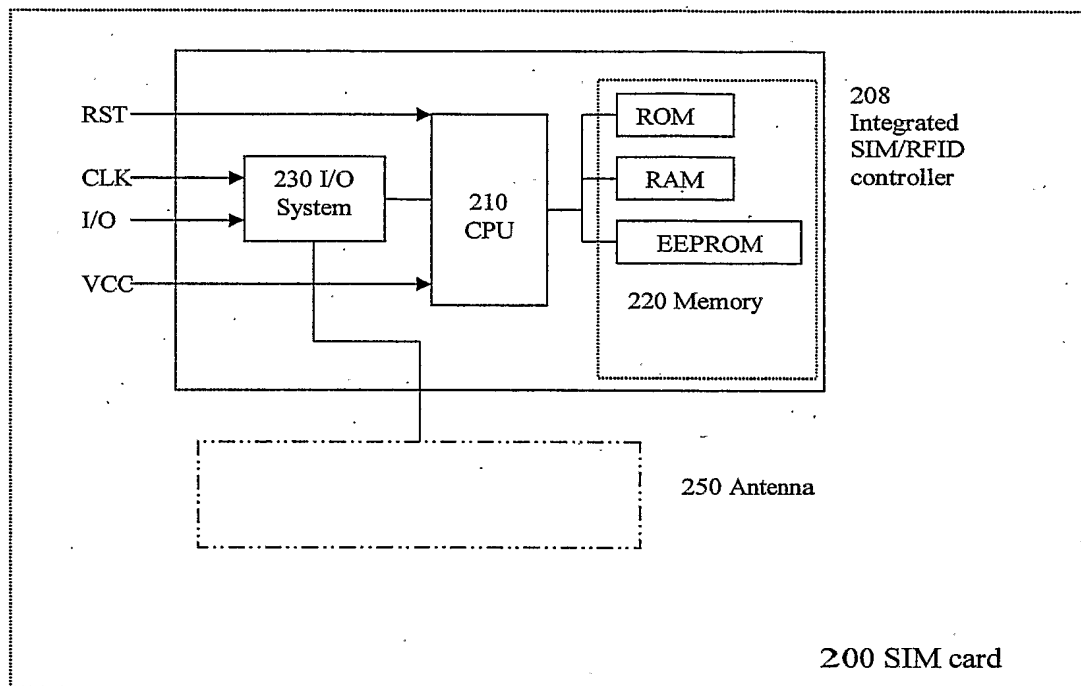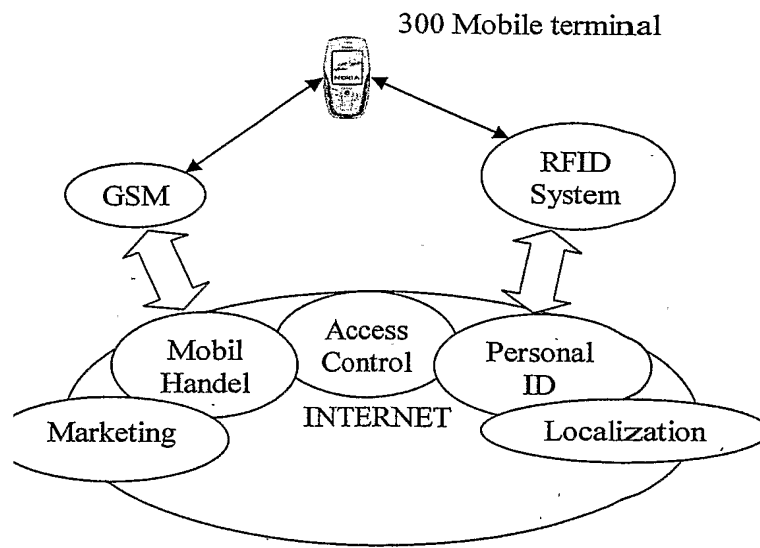
Figure 1

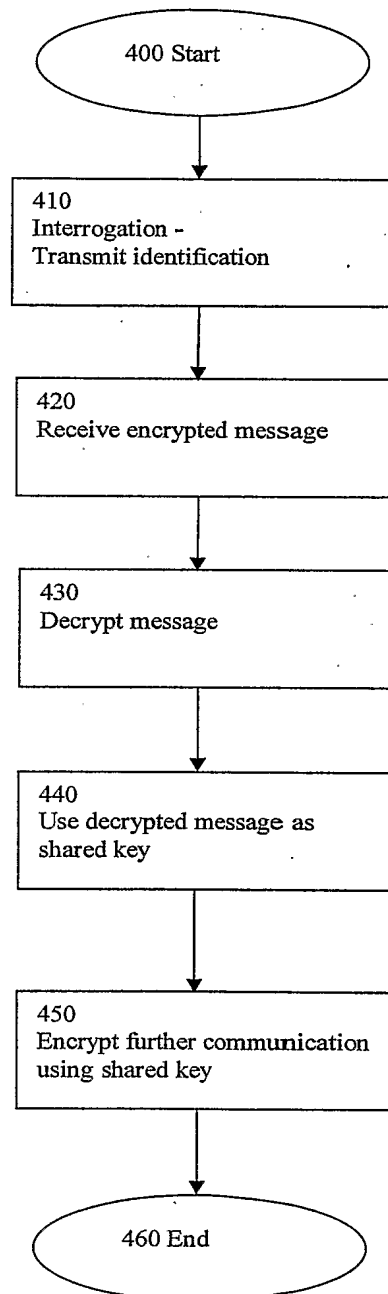**Figure 2**

Figure 3 Merging of RFID and GSM services

```
        ┌─────────────────────────┐
        │       400 Start         │
        └─────────────────────────┘
                    │
                    ▼
   ┌───────────────────────────────────┐
   │ 410                               │
   │ Interrogation -                   │
   │ Transmit identification           │
   └───────────────────────────────────┘
                    │
                    ▼
   ┌───────────────────────────────────┐
   │ 420                               │
   │ Receive encrypted message         │
   └───────────────────────────────────┘
                    │
                    ▼
   ┌───────────────────────────────────┐
   │ 430                               │
   │ Decrypt message                   │
   └───────────────────────────────────┘
                    │
                    ▼
   ┌───────────────────────────────────┐
   │ 440                               │
   │ Use decrypted message as          │
   │ shared key                        │
   └───────────────────────────────────┘
                    │
                    ▼
   ┌───────────────────────────────────┐
   │ 450                               │
   │ Encrypt further communication     │
   │ using shared key                  │
   └───────────────────────────────────┘
                    │
                    ▼
        ┌─────────────────────────┐
        │       460 End           │
        └─────────────────────────┘
```

Fig. 4
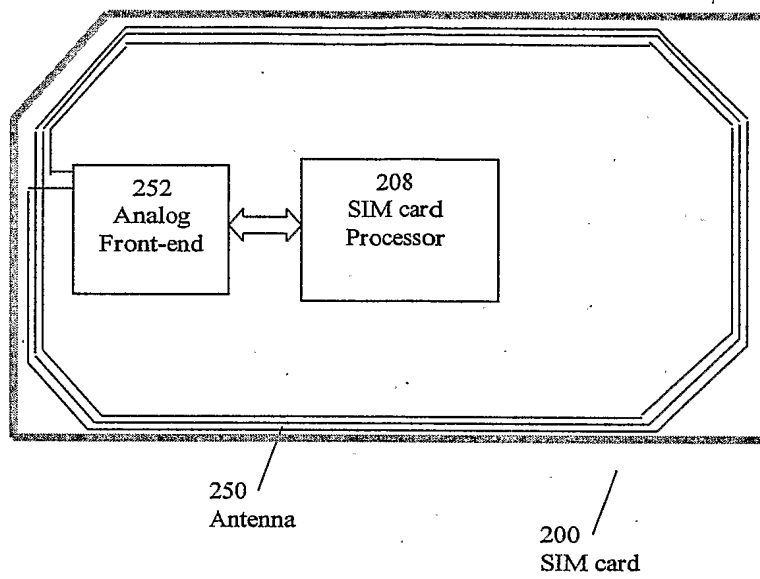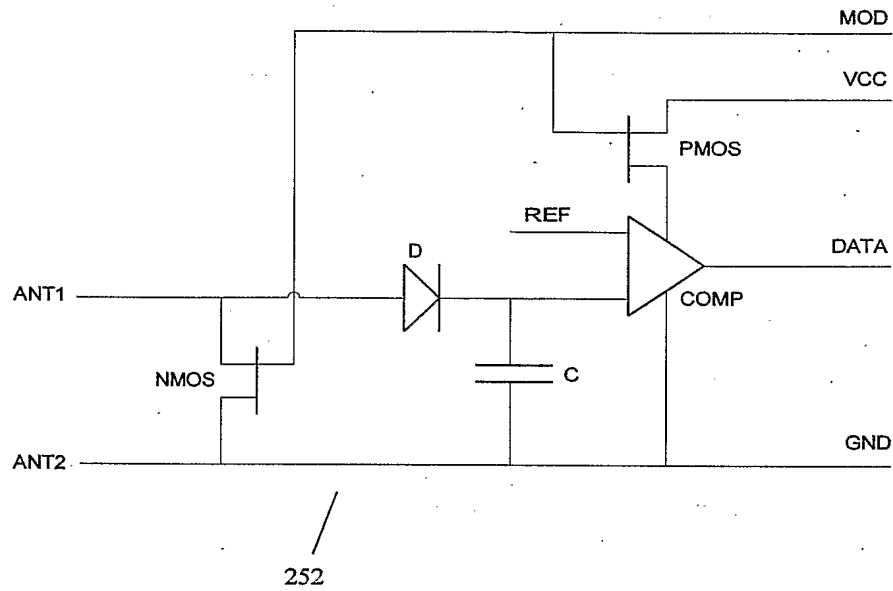
Figure 5

Figure 6

INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04Q7/32   G06K7/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04Q G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CA 2 293 393 A1 (SWISSCOM AG) 23 December 1998 (1998-12-23)	1,2,6-21
Y		3-5
	page 5, line 29 - page 6, line 1 page 8, line 9 - page 9, line 2 page 9, lines 7-17 page 10, lines 10-16 page 10, line 22 - page 11, line 21 page 15, lines 1-3 page 16, lines 11-24 -----	
Y	US 2003/006280 A1 (SEITA KAZUHISA ET AL) 9 January 2003 (2003-01-09) abstract paragraphs '0005!, '0009!, '0012! paragraphs '0030!, '0031!, '0034! paragraphs '0037!, '0052! -----	3-5

☐	Further documents are listed in the continuation of box C.	X	Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 June 2005	24/06/2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Chimet, D

Form PCT/ISA/210 (second sheet) (January 2004)

Patent document cited in search report			Publication date	Patent family member(s)			Publication date
CA 2293393	A1		23-12-1998	WO	9858509	A1	23-12-1998
				AT	215291	T	15-04-2002
				AT	212774	T	15-02-2002
				AU	736350	B2	26-07-2001
				AU	3022497	A	04-01-1999
				AU	739465	B2	11-10-2001
				AU	5649598	A	04-01-1999
				CA	2294721	A1	23-12-1998
				WO	9858510	A1	23-12-1998
				CN	1260939	A	19-07-2000
				CZ	9904270	A3	15-03-2000
				CZ	9904272	A3	15-03-2000
				DE	59706821	D1	02-05-2002
				DE	59802969	D1	14-03-2002
				DK	990355	T3	01-07-2002
				DK	990356	T3	29-04-2002
				EP	0990355	A1	05-04-2000
				EP	0990356	A1	05-04-2000
				ES	2172870	T3	01-10-2002
				HU	0003157	A2	29-01-2001
				HU	0003565	A2	28-03-2001
				JP	2002511217	T	09-04-2002
				JP	2002510444	T	02-04-2002
				NO	996145	A	16-02-2000
				NO	996148	A	11-02-2000
				NZ	501858	A	28-09-2001
				NZ	501859	A	28-08-2002
				RU	2204166	C2	10-05-2003
				RU	2212118	C2	10-09-2003
				TW	480449	B	21-03-2002
				US	6859650	B1	22-02-2005
				ID	22976	A	23-12-1999
				PT	990356	T	31-07-2002
US 2003006280	A1		09-01-2003	JP	2003016398	A	17-01-2003

PUB-NO:	WO2005096651A1
DOCUMENT-IDENTIFIER:	WO 2005096651 A1
TITLE:	TITLE DATA NOT AVAILABLE
PUBN-DATE:	October 13, 2005

ASSIGNEE-INFORMATION:

NAME COUNTRY